International
Comparative
Legal Guides

Digital Health 2021

A practical cross-border insight into digital health law

Second Edition

Featuring contributions from:

Advokatfirma DLA Piper KB
Arthur Cox LLP
Astolfi e Associati, Studio Legale
Baker McKenzie
Bird & Bird LLP
Cliffe Dekker Hofmeyr
Consumer Technology Association (CTA)
D'LIGHT Law Group
Deloitte
Gilat, Bareket & Co., Reinhold Cohn Group
GVA LPC
Hammad and Al-Mehdar Law Firm
Haynes and Boone, LLP
Herbst Kinsky Rechtsanwälte GmbH
Johnson & Johnson
KYRIAKIDES GEORGOPOULOS LAW FIRM
Lee and Li, Attorneys-at-Law
LexOrbis
Llinks Law Offices
Machado Meyer Sendacz e Opice Advogados
McDermott Will & Emery AARPI
McDermott Will & Emery LLP
NeuroPace, Inc.
OLIVARES
Quinz
VISCHER

ICLG.com

ISBN 978-1-83918-097-2
ISSN 2633-7533

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2021

Second Edition

Contributing Editor:
Roger Kuan
Haynes and Boone, LLP

©2021 Global Legal Group Limited.
All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

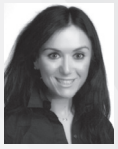
Introductory Chapters

Expert Chapters

Q&A Chapters

Key Considerations in a "It's All About the Data" Healthcare World


Jason Novak


Irina Ridley

Haynes and Boone, LLP
NeuroPace, Inc.

Introduction

In the beginning, there were two disparate worlds. One world was the healthcare industry. The other was the tech industry. And then, in a moment, these two worlds converged and a new approach to delivering healthcare was born. Digital health emerged to address a continuously growing technological gap in a historically stagnant industry through systems and tools that had long been used to make other industries better. This focus on innovation allowed various health sectors to start benefitting from artificial intelligence and cloud-based technologies (e.g., machine leaning, internet of things, data analytics, graphic user interfaces, and blockchain), aligning them with the industry's main mission by being able to better diagnose disease, manage illness, manage health risk, and promote general wellness. As this new world of digital health grew, and continues to grow, a solar system has emerged, one with various sectors within digital health. These sectors include, for example, mobile health, health IT, telehealth/connected health, virtual health, telemedicine, interoperability platforms, personal genomics, health and wellness applications, advanced medical imaging platforms, electronic health and medical record technologies (EHR/EMR), and so on. (The same could be said for the convergence of tech and biotech to form new digital platforms for precision medicine, drug discovery, digital therapeutics, computational biology, and so on. But that is a topic for another day.)

Digital health will continue manifesting throughout the healthcare industry. If COVID-19 has taught us anything, it is that companies, healthcare providers, and healthcare systems that have figured out how to maintain a digital infrastructure are nimbler and more capable of adapting to changes in healthcare delivery while driving adoption for the same. Given that reality, regardless of how complex our newly redesigned healthcare industry may get, there is a common theme: data is king and the proper generation, acquisition, maintenance, transaction and/or use of data is essential to a successful digital health endeavour. As a result, to continue being relevant and adapting to the new operating reality, companies must focus on establishing a well-developed data strategy to execute a digital health endeavour.

Why Data Strategy Matters

"Blind spots"

First, as a baseline, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters issues unique to their industry. For example, the tech industry deals with data transactions, data privacy, and cybersecurity on a regular basis. Healthcare traditionally has not (not until digitisation brought about the concept of using and transacting with personal health information under HIPAA and other laws, which we will discuss later). Healthcare must contemplate FDA oversight and reimbursement considerations on a regular basis, while tech traditionally does not. Therefore, these industries have historically functioned in parallel – with tech focusing on fast-paced development and reinvention to create the best, most innovative products, and healthcare, which is extremely highly regulated and appropriately risk averse, concentrating on assessing every potential consideration before implementing a change. Given that digital health is a combination of both, it is often the case that most entities in the digital health world will have strategic (often legal) "blind spots" based on their experience leading up to an endeavour.

Use requirements

Second, healthcare data is exceptionally valuable for both the patient and the company that is able to procure such data. Given its criticality, one must have permission to use healthcare data for a desired purpose. Regardless of whether the healthcare data is generated or acquired by the data user, the data user must have the consent of the data's ultimate owner, i.e., the patient, to use that healthcare data. In cases where healthcare data is acquired from a third party, the data user must also have the consent of the third party to use the healthcare data for a desired purpose. Often, consent from a third party (e.g., a healthcare data warehouse or aggregator) comes in the form of a data transaction, whereby said data user will usually remunerate the third party to acquire the healthcare data for the desired purpose. Of course, the consent between data owner and data user will come via the data owner providing consent to this third party to transact the data to parties such as the data user. It is worth noting that a healthcare data warehouse or aggregator does not solely mean data mines such as those used by personal genomics companies, e.g., 23andMe and Ancestry.com. It also includes traditional entities such as hospitals and hospital systems, universities, research institutes and pharmaceutical companies. For simplicity, we will refer to these types of entities as Healthcare Data Aggregators (HDAs). Consent can come in a variety of ways, but it is critical to be able to demonstrate such consent for any downstream data use.

Transacting with sophisticated entities

Third, as introduced above, healthcare data is usually acquired from the HDA, through a data transaction, looking to benefit from their held healthcare data. A benefit to a HDA can be in the form of, for example, direct remuneration, royalties from

© Published and reproduced with kind permission by Global Legal Group Ltd, London

data user revenue, milestone payments (commercial and revenue milestones), equity in the data user's company, and access to the data user's analytical results. In cases where both parties are subject to some form of collaboration, joint venture or co-development agreement, profit can also include some ownership of co-developed intellectual property with the data user.

Moreover, given that most HDA entities are likely to be large and traditionally sophisticated, negotiation leverage can be skewed in the HDA's favour. However, as discussed above, depending on the type of HDA, the sophistication may not carry to data transactions.

On the one hand, a personal genomics HDA builds their business model around these transactions and therefore is very experienced at data transactions. In fact, some may have fairly set terms determined over time and experience, and therefore leave little room for negotiation. On the other hand, some traditional entities (hospitals, universities, research institutes, big pharma) may have general sophistication, but that may not stretch to data transactions. For example, being a sophisticated healthcare research institute does not inherently mean that said institute has any deep experience in healthcare data transactions. Additionally (and noteworthy), these sophisticated entities often operate amidst internal silos, where the portion of the organisation generating data may not be the same group that understands its value, understands what parameters exist around these data (e.g., consent limitations), and has business acumen to transact on these data. Since digital health is a convergence of typically disparate industries, as discussed above, "blind spots" can exist for even the most sophisticated entity.

Executing multiple transactions

Fourth, robust healthcare data sets may have to be acquired through multiple transactions. The most robust healthcare data set, depending on what one is researching, will be heterogeneous as to race, sex, age and so on. A one million genome data set is nice, but the set is less valuable when it comes from one country of predominantly one race. The United States is home to various robust heterogeneous data sets. The United Kingdom, through their recently announced UK Genomics Initiative, is another country with a path to robust heterogeneous data sets. There are other smaller examples, but these are few. As a result, a party looking to possess and analyse a robust data set for a particular reason may need to execute multiple data transactions, often cross-border, to cobble together a sufficient data set. Several issues arise with this.

One obvious issue of multiple transactions is cost to the company. As discussed above, HDAs look to benefit through several means. Multiple transactions may be needed which, if not careful, can drastically and negatively impact the data user's ability to appropriately scale the product offering born out of the analysis of these data sets. Each counter-party to a data transaction may want their respective portion of equity, royalties, milestones and so on. Each counter party may push for intellectual property rights generated resulting from the data use. These agreements, taken together, can saddle a data user company (e.g., digital health company) with significant financial responsibilities to multiple third parties. This can obviously impact an investor's perception of the viability of such a company and ultimately the utility and value of the products or services they are offering (coming full circle and limiting the industry's ability to benefit from technology and innovate accordingly).

Another issue is time and resources. Each transaction takes time. Each transaction cannot necessarily be handled concurrently with other transactions, as earlier transactions may form the base terms that guide subsequent transactions. As a result, properly securing a robust data set can extend for months. On the other hand, if a data user desires to handle transactions concurrently, then resources can become an issue as each transaction demands committed headcount and finances. Such a commitment, particularly for smaller companies, may not be possible with limited human resources and strapped cash flow, both inherent to many smaller companies.

Heavy regulation

Fifth, healthcare data is heavily regulated. Various national laws related to data privacy exist, as well as specific laws related to personal health information. While there are national data privacy laws for healthcare, such as HIPAA, each state has their own data privacy laws (e.g., the CCPA in California). Moreover, countries have their own data privacy laws (e.g., the GDPR in the EU). Oftentimes, these laws have conflicting requirements and given how quickly they are being passed, it is impossible to benefit from reviewing prior enforcement actions or looking for precedent. Navigating either the national and/or international legal landscape therefore requires sophisticated legal expertise, often in the form of multiple international firms working in tandem, particularly to navigate cross-border transactions. Of course, with this comes additional cost and time beyond the time and resources to handle multiple transactions in the first place.

Failure is death

Sixth, data is often the backbone to a digital health company as it typically drives and supports the platform/product offering. Data can be used, for example, to train an artificial intelligence or machine learning engine used for various digital health constructs such as an imaging analytics software product. Regardless of where that data is generated, consent by the data owner is required to use data not only for commercial and marketing purposes, but also for R&D and product improvement, either directly or through a third-party data warehouse or aggregator. If such consent or rights is not obtained appropriately, the use of that data may not be legal. As such, the time, cost and resources to train an artificial intelligence or machine leaning engine may be wasted, delaying product development and eventual product launch, not to mention burning through financial resources that may be tightly finite particularly for smaller companies. Of course, the reputation risk and customer trust impact surrounding misuse of data may be the biggest killer of all.

Fundamentals of Data Rights Protection/ Transaction

The preceding should instill how important data rights and privacy are from the get-go, and how your business plans can be severely impacted if a data strategy is not set up appropriately. Data strategy therefore must be treated with its due respect, as it can be the lifeblood for companies emerging in the digital health space as well as organisations that are interested in incorporating digital health tools and health tech offerings to better their own offerings. With that, let us investigate some of the fundamental considerations of data rights protection and transaction.

Core data strategy questions

First off, one should ask some core questions to help define the data strategy.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

1. What is the intended purpose of data? Defining this purpose early and often is essential as it will become core to the metes and bounds of the data transaction and will help with the initial undertaking of seeking appropriate (patient) consents, which is far easier to do at the outset.
2. What are potential secondary uses of the data? Defining secondary purposes up front is also important as a data user must maximise the value of the data transaction. Failing to set the expectation early may result in a data transaction of limited scope, forcing a data user to either seek amendment to the existing transaction or the need for a second agreement. In either case, leverage in negotiation will quickly pivot to the data holder, who will now have a clear idea of the importance to the data user of these secondary users.
3. Where is the data coming from and where is it going? To answer this, detailed data maps need to be developed, tracing the path of data across various states and nations, thereby identifying the jurisdictions that will define the scope of data compliance requirements for a data user. As stated above, each impacted territory, whether state or country, may have unique data compliance (data privacy) laws that must be accounted for in executing the data strategy. Of note, data mapping is a requirement under several of the potentially applicable healthcare laws, so this actually factors into several parts of the data strategy.

With these goalposts in place as to data need and territories impacted, compliance requirements can be established, data transactions can be executed, and then product development can commence.

Compliance considerations

At a high level, data compliance can typically involve HIPAA for US healthcare data, other US federal laws related to general data privacy, US state data privacy laws, and ex-US data privacy laws. As the various data privacy laws are too numerous to enumerate and discuss in detail herein, the following will tackle some of the high-level questions one should ask related to HIPAA.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the fundamental US federal law related to protecting health information. HIPAA breaks down into five separate rules, those being the Privacy, Security, Transactions, Identifiers, and Enforcements Rules. Of those, the Privacy and Security Rules generally garner the most attention as these are directed to protecting the privacy and security of individually identifiable health information. In particular, the Privacy Rule deals with protected health information (PHI). The Security Rule covers the protection of electronic health information (ePHI).

In dealing with HIPAA, a threshold determination is whether one is an entity subject to HIPAA (referred to as a "Covered Entity"), or a "Business Associate" of said Covered Entity by way of providing certain services for the Covered Entity. Covered Entities, aside from providers of healthcare that bill through claims, include, for example, government healthcare programmes (e.g., Medicare, Medicaid, military health programmes, veteran health programmes), health maintenance organisations (HMOs), employee sponsored health plans, and health insurance companies. Business Associates are parties (person or entity) that are not part of a Covered Entity workforce but, by virtue of acting on behalf of or providing certain services to a Covered Entity, receive access to PHI that is in the possession of the Covered Entity and for which the Covered Entity is responsible.

So, what constitutes PHI? HIPAA provides 18 specific identifiers that turns health information to PHI. If one or more of those identifiers are present, then the information is PHI subject to HIPPA's rules. To avoid running afoul of HIPAA guidelines when PHI is in play, one can de-identify the data or transact only for de-identified data. Under HIPAA's Privacy Rule, data can be de-identified by expert determination or by safe harbour, the latter being by removal of the aforementioned identifiers and by having no actual knowledge that residual information can be used to identify the individual. It should be noted that de-identification is not a risk-free solution, as either path for de-identification does not guarantee that de-identified data cannot be re-identified, therefore pulling all of HIPAA's restrictions back into play.

The better solution is to anonymise the data. As opposed to de-identification, anonymisation involves irreversibly breaking all links between the person and the associate health record such that re-identification is practically impossible. As such, any ties to HIPAA also would break.

Transact first, develop second

With a sound data and compliance strategy in mind, and with walkaway terms in place (we cannot forget about those), one is better prepared to execute a data transaction. With a sound data and compliance strategy, one will understand the path that data will travel, the corresponding compliance requirements, and the desired primary and secondary uses for that data that should come with the transaction. With a sound data and compliance strategy, one can also be better positioned to account for the necessary compliance, confidentiality and consent requirements associated with the data, as well as one's own likely categorisation as a Covered Entity or Business Associate bound by HIPAA.

Finally, and just as important as all that precedes, with proper data transactions in place, one is now ready to develop a digital health offering with the benefit of the data that has been secured. As stated above, by appropriately setting the stage for development, one can avoid the well-worn path of fast-paced reinvention that is so common in the tech industry, all the while protecting the company from data rights issues that could lead to lost time, resources, and money, thereby negatively impacting investor confidence. This approach will help ensure the viability of the product offering that is so critical in the healthcare setting.

This new and rapidly expanding world of digital health has provided, and will continue to provide, exciting new opportunities for delivering better, more efficient, and more accurate health offerings to patients. With a new normal in place now and into the near future, digital health capabilities will continue to serve a vital role, facilitating new technologies that emerge from a growing acceptance and adoption of technology into the healthcare paradigm. With this will come new regulatory requirements, additional scrutiny, and a relentless focus on weeding through the complexities.

To remain successful, as with adapting to COVID-19, companies and organisations need to act quickly (but carefully) to keep up. But companies and organisations must operate with the understanding that, putting oneself on the fast track to digital health success requires an upfront and sophisticated data and compliance strategy to minimise the number of barriers that could impede that success. Allotting the time and resources to do this correctly from the outset will be critical to that success. Finally, with increasing competition in the digital health space, differentiation is essential. That differentiation need not come solely from product features, but also can come from communicating a sophisticated plan to ensure the data one uses or generates does not create unnecessary legal issues down the road and maintains the confidences of the users and ultimately the patients. Good luck!

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Jason Novak is a Partner in Haynes and Boone's Precision Medicine and Digital Health Practice Group, where he focuses on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare and life sciences industries. Tech and biotech are traditionally disparate technologies that, when blended together to form many of our most exciting new technologies, bring forth a combination of unique and interrelated legal issues. Jason has extensive experience in IP strategy and patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management, and dispute resolution. Prior to starting this practice, Jason was an IP Director for Thermo Fisher Scientific, where he managed worldwide IP needs in genetic sciences instrumentation and software.

Haynes and Boone, LLP
201 Spear Street, Suite 1750
San Francisco, CA 94105
USA

Tel: +1 650 687 8800
Email: jason.novak@haynesboone.com
URL: www.haynesboone.com

Irina Ridley is a seasoned healthcare attorney with deep business expertise. Irina joined NeuroPace as General Counsel and Corporate Secretary in November 2020. Prior to NeuroPace, she oversaw Legal at Myriad Women's Health, a precision medicine company. She joined Myriad, by way of acquisition in July 2018, and served as Chief Counsel.
Prior to Myriad, Irina was Associate General Counsel at Counsyl, Inc., where she oversaw several financings and market checks, an IPO process, and finally the acquisition by Myriad. She was also responsible for corporate governance, strategy and partnerships, and served as Counsyl's Privacy Officer. Irina has held leadership positions at and advised companies in device, pharma, biotech, digital health, and diagnostics. She received her Bachelor's of Science degree, *cum laude*, from Rensselaer Polytechnic Institute, where she also earned her MBA, *summa cum laude*, and her law degree, *summa cum laude*, from Albany Law School.

NeuroPace, Inc.
455 N. Bernardo Avenue
Mountain View, CA 94043
USA

Tel: +1 650 237 2700
Email: iridley@neuropace.com
URL: www.neuropace.com

Haynes and Boone, LLP is an international corporate law firm with offices in California, Charlotte, Chicago, Denver, London, Mexico City, New York, Shanghai, Texas, and Washington, D.C., providing a full spectrum of legal services in energy, technology, financial services and private equity. With more than 575 lawyers, Haynes and Boone is ranked among the largest U.S.-based firms by *The National Law Journal*, *The American Lawyer* and *The Lawyer*. It also was recognised across the board for excellence in the BTI Consulting Group's 2020 "A-Team" report, which identifies the law firms that in-house counsel commend for providing superior client service.

www.haynesboone.com

haynesboone

© Published and reproduced with kind permission by Global Legal Group Ltd, London

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group